# REPORT OF INVESTIGATION

| | |
|---|---|
| File Number: | 03-093 |
| Agency: | Georgia Technology Authority (GTA) |
| Basis for Investigation: | Inspector General Initiated |
| Allegations: | Inappropriate Computer Use |
| Date Opened: | March 11, 2003 |
| Investigated By: | Deborah Copeland<br>Deputy Inspector General |
| Date of Report: | January 7, 2004 |

# OFFICE OF THE INSPECTOR GENERAL

## File Number: 03-093

## EXECUTIVE SUMMARY

The Office of Inspector General (OIG) initiated an inquiry concerning potential instances of inappropriate use of state-owned computer hardware and software by state employees. Management officials of the Georgia Technology Authority (GTA) worked closely with the OIG to examine policies and practices surrounding this issue which includes computer network access and usage as well as Internet and email usage. The GTA is charged with setting the direction for the state's use of technology that affects over 65,000 computer users statewide. Individual agencies may establish more stringent policies and procedures consistent with the GTA Enterprise Policy and associate Standards.

The GTA conducted an in-depth review of usage and analyzed the data. Statistics derived from the data did not suggest a problem significant enough to continue investment of resources into this area. Therefore, the GTA and the OIG focused on other more global facets of this issue geared to various preventive measures. These included: 1) written communication and dissemination of the appropriate use policy to agency heads asking for their assistance in enforcement; 2) news articles written to increase state employees' awareness and understanding of the state's policy; and 3) a survey of other states' policies focusing on encountered problems and associated corrective measures they may have implemented.

Employee awareness through dissemination of GTA's policy 3.1.3 "Appropriate Use of Information Technology Resources" helps minimize the cost of security incidents and assure the consistent implementation of controls for information systems throughout the state. As with any state policy, all users (employees, contractors, vendors, and other parties) are expected to understand and abide by the parameters set forth therein.

Based on the findings, the OIG recommends that agencies employee the use of warning banners (to the extent practical and permissible by law) to warn authorized and unauthorized users that 1) the system is a government computer system; 2) what is considered proper use of the particular system; and 3) that there is no express or implied expectation of privacy while using the system. Ideally, such banners would be part of standard log-on procedures; however, alternatives such as stickers or labels affixed to monitors may also be used.

**Report of Investigation** **File No. 03-093**

# TABLE OF CONTENTS

# SUMMARY OF ACTIONS
# File: 03-093

## I. BASIS FOR INVESTIGATION

The Office of the Inspector General (OIG) initiated an inquiry concerning potential instances of inappropriate use of state-owned computer hardware and software by state employees. Management officials of the Georgia Technology Authority (GTA) worked closely with the OIG to examine policies and practices surrounding this issue which includes computer network access and usage and Internet and email usage.

## II. NARRATIVE

In the Spring of 2003, the OIG launched this inquiry after the Georgia Bureau of Investigation conducted a criminal investigation into allegations that a Georgia Department of Education employee had utilized his department laptop to download pornography from the internet. The employee was arrested and charged with 73 counts of violation of sexual exploitation of children. Due to the fact that the employee was employed by the state and utilized state computer equipment for the commission of a crime, the case was prosecuted by the Attorney General's office.

The OIG contacted GTA Director Tom Wade to obtain assistance in the examination of state policies and actual practices surrounding the issue of inappropriate use of computers. GTA is charged with setting the direction for the state's use of technology that affects over 65,000 computer users statewide. Individual agencies may establish more stringent policies and procedures consistent with the GTA Enterprise Policy and associate Standards. In fact, some agencies already employ various blocking software programs which help prevent this type of abuse. Director Wade explained in detail GTA's existing policy 3.1.3 of September 10, 2002, entitled "Appropriate Use of Information Technology Resources." The policy clearly states, "State of Georgia information technology resources are provided to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused." He also provided an overview of certain technical issues GTA encounters and outlined four areas of concern specific to existing GTA software that is capable of tracking inappropriate usage. He explained the State's Intrusion Detection System used to detect hacking and other attempts to breach security on the state network, which has the capability of detecting inappropriate use. Additionally, he advised that GTA has considered more specific filtering software programs that would eliminate "a high percentage" of access to inappropriate Internet sites. This program would cost the state about $400,000 and would involve requests for additional staffing. Given the State's budget, this avenue has not been aggressively pursued.

Director Wade agreed to assist the OIG by conducting an in-depth review of usage which would reveal instances of inappropriate use. Subsequently, the OIG and GTA jointly reviewed the information/statistics identified during the review. Of the 68,000+ work stations accessing Internet websites on multiple occasions, it was noted that only a very slight percentage of .9 of the addresses actually accessed by users revealed potential inappropriate access. However, even this statistic can be skewed due to “false positives”, firewall configuration, and other variables. A more In-depth analysis is possible and can be carried out; however, it is very time intensive and requires well trained IT staff members who can ensure all variables are considered. The actual statistics derived from the aforementioned analysis did not suggest a problem significant enough to continue investment of resources into this area.

## III. CONCLUSION

At the time of the inappropriate use analyses, the actual statistics that GTA derived from a thorough examination of data did not reveal and/or suggest a problem significant enough to continue investing IT resources to facilitate the furtherance of the investigation. Therefore, GTA and the OIG began to focus on other more global facets of this issue geared to various preventive measures. These included: 1) news articles written to increase state employees’ awareness and understanding of the state’s policy; 2) written communication and dissemination of the policy to agency heads asking for their assistance in enforcement; and 3) a survey of other states’ policies focusing on encountered problems and associated corrective measures they may have implemented.

Noncompliance with the state policy on “Appropriate Use” may constitute potential risks to the State of Georgia’s information technology. Therefore, all agency heads should endeavor to continuously promote individual employee awareness and compliance with GTA’s policy 3.1.3 “Appropriate Use of Information Technology Resources.” Employee awareness through dissemination of this policy helps minimize the cost of security incidents and assure the consistent implementation of controls for information systems throughout the state. All users (employees, contractors, vendors, and other parties) are expected to understand and abide by this and other state policies.

## IV. REFERRALS

There are no referrals relating to this complaint.

## V. RECOMMENDATIONS

Based on our findings, the OIG recommends that agencies employ the use of warning banners (to the extent practical and permissible by law) to warn authorized and unauthorized users of the following:

1. That the system they are using is a government computer system
2. what is considered the proper use of that particular system, and
3. that there is no express or implied expectation of privacy while using the system.

The wording of the banner should be consistent with the Appropriate Use of Information Technology Resources policy (policy number 3.1.3) in GTA's Enterprise Information Security Policies, which can be found in the Policies & Standards section of GTA's website at http://gta.georgia.gov.
Ideally, such banners would be part of standard log-on procedures; however, alternatives such as stickers or labels affixed to monitors may also be used.